Meridian 1

Basic and Network Authorization Code

Description

Document Number: 553-2751-103
Document Release: Standard 7.00
Date: April 2000

Copyright ©1990–2000 Nortel Networks
All Rights Reserved

Printed in Canada

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant. This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC rules, and the radio interference regulations of the Industry Canada. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case users will be required to correct the interference at their own expense.

SL-1 and Meridian 1 are trademarks of Nortel Networks.

Revision history

April 2000

Standard 7.00. This is a global document and is up-issued for X11 Release 25.0x.

October 1997

Standard 6.00.

July 1995

Standard 5.00. This document is issued to include X11 Release 21 changes.

December 1994

Standard 4.00. Reissued to include editorial changes and indexing.

August 1993

Standard 3.00. This document is reissued for updates and changes resulting from X11 Release 19.

December 1991

Standard 2.00. This document is reissued to include technical content updates.

August 1990

Standard 1.00. Reissued for compliance with Nortel Networks standard 164.0.

Contents

Introduction 7
Reference list 7
Document overview 8
Other documentation 8

Feature description 9
Reference list 9
Basic Authorization Code 9
Authorization code validation 10
Station Specific Authcode 10
Authcode security enhancements 11
Collect Call Blocking(Brazil) 15
Direct Private Network Access 24
Electronic Lock Network Wide/Electronic Lock on Private Lines . 32
Three-Wire Analog Trunk -
Commonwealth of Independent States (CIS) 37
Authorization code administration 61
Network Authorization Code 62
Authorization code conditionally last 62
Attendant input of authorization code 63

Operating parameters 65

Feature interactions 67
Feature key operations 67
Call Detail Recording 69

Authcode input via tie trunks 69
Direct Inward System Access 69
Barge-In or Busy Verify 69
Centralized Attendant Service 70
Call Forwarding 70
Network Class of Service 70
Network/Basic Alternate Route Selection 70
Network Queuing 70
Coordinated Dialing Plan 71

Implementation 73
Reference list 73

Feature operation 79
Authcode after SPRE 79
500/2500/SL-1 or digital telephones 79
Attendant 80
Authcode conditionally last 80
Invalid authcodes 80

Packaging 81

List of terms 83

Index 85

Introduction

Reference list

The following are the references in this section:

- *Basic and Network Alternate Route Selection Description (553-2751-100)*
- *Coordinated Dialing Plan Description (553-2751-102)*

The Basic and Network Authorization Code features enable selected users to temporarily override the access restrictions assigned to a station or trunk. A user can enter an authorization code (authcode) to access more of the system facilities than would normally be allowed to the particular station or trunk because of the assigned Network Class of Service (NCOS), Class of Service (COS), and Trunk Group Access Restriction (TGAR) codes.

These features are useful when a user initiates a call from someone else's telephone and requires access to more system facilities (such as access to long distance calling) than are allowed to that telephone. Entering a valid authorization code enables the user to access these additional features. After a valid authorization code is entered, the NCOS, COS, and TGAR associated with the authorization code replace the NCOS, COS, and TGAR associated with the telephone for the duration of the call.

Station Specific Authcode (SSAU) is a special feature available with X11 release 19 that enables the system administrator to control the level of authorization code access on a per telephone basis.

Starting with X11 release 21, the following features are available:

— Authcode Security enhancements provides Authcode alarm when invalid Authcode entry is detected.

— Collect Call Blocking (Brazil) provides a mechanism for special treatment of incoming DID and CO collect calls on 2 Mbit/sec digital trunks and analog trunks. This feature is provided on a route and individual user basis.

— Direct Private Network Access provides for DISA Digit Insertion where 1-31 digits can be automatically inserted for a DISA call, DISA RAN where a DISA caller can be greeted by a recorded announcement, and Authcode-last Retry where a caller can be reprompted for Authcode if the first Authcode entered for Authcode-last is invalid.

— Electronic Lock Network Wid/Private Lines enhances the current Electronic Lock capability over the network and extends the coverage of electronic lock to include private line DNs.

— Wire Analog Trunk for CIS provides the capability to adapt the Meridian 1 to three wire analog trunks used in the CIS market.

Document overview

This publication describes the authorization code features as offered on the following X11 software:

— Basic Authorization Code (BAUT) for general applications

— Network Authorization Code (NAUT) for network applications

Other documentation

Other Nortel Networks technical publications (NTPs) related to BAUT and NAUT are as follows:

— *Basic and Network Alternate Route Selection Description (553-2751-100)*

— *Coordinated Dialing Plan Description (553-2751-102)*

Feature description

Reference list

The following are the references in this section:

- *Basic and Network Alternate Route Selection Description (553-2751-100)*
- *Coordinated Dialing Plan Description (553-2751-102)*

Basic Authorization Code

Basic Authorization Code (BAUT) (package 25) provides for up to 4096 authorization codes of 1 to 14 digits. Users can enter an authorization code after dialing the Special Prefix (SPRE) and the digit "6" before dialing any call, including a Network Alternate Route Selection (NARS), Basic Alternate Route Selection (BARS), or Coordinated Dialing Plan (CDP) call. With the BAUT feature, an authorization code can be entered when doing the following:

— originating a call from a local station or tie trunk

— initiating a call transfer or conference from a local station

— originating a call via the Direct Inward System Access (DISA) feature

Note: Refer to *Basic and Network Alternate Route Selection Description (553-2751-100)* for a description of the NARS and BARS features. Refer to *Coordinated Dialing Plan Description (553-2751-102)* for a description of the CDP feature.

Authorization code validation

The software validates an entered authorization code on the basis of the number of digits dialed and the dialed digits themselves. If the number of digits in the entered authorization code does not match the defined authorization code length (authorization code Data Block, AUB, LD 88), the authorization code is deemed invalid. Similarly, if the dialed authorization code digits are not defined in the authorization code table (AUT, LD 88), the authorization code is deemed invalid.

When an invalid authorization code is encountered, no response is given to the user until the End-of-Dialing (EOD) timer expires. (This increases the security of authorization codes by making it difficult for an unauthorized user to determine the length of a valid authorization code.) When the EOD timer expires, overflow tone is given for 15 seconds and the call is forcibly disconnected.

Station Specific Authcode

With X11 release 19 and later, Station Specific Authcode (SSAU), package 229, enables the system administrator to define the authorization code access level for each telephone. This feature applies to 500/2500 and digital telephones and is implemented on a per telephone basis. It does not apply to BRI telephones.

Station Specific Authcode provides three levels of authorization code access:

1 AUThcode Unrestricted (AUTU)
A telephone configured as AUTU has no authorization code access limitations.

2 AUThcode Restricted (AUTR)
A telephone configured as AUTR can enter up to six assigned authorization codes. (The same authorization code may be assigned to more than one AUTR telephone.)

3 AUThcode Denied (AUTD)
A telephone configured as AUTD has no access to authorization codes. Any authorization code entered will be rejected, and the call will not be completed.

Operating parameters

The same authorization code may be assigned to more than one AUTR telephone.

There is cross-checking between LD 10 and LD 11, which define a station specific authorization code, and LD 88, which ensures that the user has entered a valid authorization code.

LD 88, which deletes an existing authorization code, does not check if the authorization code is assigned as a station specific authorization code before the deletion.

Attendant Administration does not support the assignment of Station Specific Authcode.

Feature operation

After an authorization code is entered, the Station Specific Authcode feature determines if the telephone is allowed to use the entered code. If the authorization code is not allowed on that telephone, the existing invalid authorization code treatment occurs. Otherwise, normal authorization code processing occurs.

Authcode security enhancements

The Authorization Code Security Enhancements feature enables a user to temporarily override the access restrictions assigned to a station or trunk because of their assigned Network Class of Service (NCOS), Class of Service (COS), and Trunk Group Access Restrictions (TGAR) codes. If a user requires access to system facilities in addition to that allowed on the set, the Authcode feature can be used to provide them.

The Authorization Code (Authcode) Alarm feature alerts the technician when an invalid Authcode is entered by generating an Authcode Alarm. The Alarm indicates to the technician that some unauthorized person may be trying to use an Authcode to illegally access the switch.

The Authcode alarm is generated upon detection of violation of all Authcode related features (i.e., Basic Network, and Station Specific Authorization code features), except for calls originated by the attendant.

A new class of alarm has been added (Security Administration - SECA) to distinguish security violations from other types of system messages. The message SECA0001 will be printed on the TTY.

Operating parameters

This feature is enabled through the Authcode data block in LD88.

The Authcode Alarm feature does not apply to calls originated by an attendant.

All existing operating parameters relating to Authorization Code usage apply to this feature.

All existing operating parameters relating to Fault Management apply to this feature.

For security reasons, the SECA0001 alarm should not be configured in the Exception Filter table.

Feature interactions

Authorization Code Features A Security Administration (SECA) message will be printed to the configured Maintenance Terminal (MTC), Filtered Alarm Output (FIL) console and/or the configured History File when an invalid Authcode is detected. The following features relate to Authorization Codes and are thus impacted: Basic Authorization Codes; Network Authorization Codes; Authcode Conditionally Last; Direct Inward System Access with Authorization Code; Station Specific Authcode; Speed Call/Autodial with Authorization Codes; Call Forward with Authorization Codes; Scheduled Access Restrictions with Authorization Codes; Coordinated Dialing Plan with Authorization Codes; and Flexible Feature Code with Authorization Codes.

Direct Private Network Access with Authorization Code Retry Only when an Authcode retry fails will a SECA message be printed to the configured MTC, FIL console and/or the configured History File.

Feature packaging

This feature is part of base X11 system software.

The following software packages are optional, but may be needed depending upon the application:

— Meridian 1 Alarm Filter (ALRM_FILTER) package 243

— Basic Authorization Code (BAUT) package 25

— Basic Alternate Route Selection (BARS) package 57

— Network Alternate Route Selection (NARS) package 58

— Coordinated Dialing Plan (CDP) package 59

— Direct Private Network Access (DPNA) package 250

— Direct Inward system Access (DISA) package 22

— Network Class of Service (NCOS) package 32

— Network Authorization Code (NAUT) package 63

— Station Specific Authcodes (SSAU) package 229

— Recorded Announcement (RAN) package 7

— Scheduled Access Restrictions (SAR) package 162, and

— System Speed Call (SSC) package 34, or Network Speed Call (NSC) package 39.

Feature implementation:

LD 88—Configure the Authcode Alarm for each customer

REQ	NEW CHG	Configure or change.
TYPE	AUB	Authcode Data Block.
CUST	0-99	Customer number.
SPWD	xxx	Secure data password.
ALEN	1-14	Number of digits in Authcode.
ACDR	(NO) YES	(Do not) activate CDR for authcodes.
AUTHCOD_ALRM	(OFF) ON	(Disable) enable Authcode Alarm.

LD 17—Configure the Alarm Filter table as per existing configuration procedures. The Authcode alarm must be configured in this table in order for the messages to be displayed on the FIL TTY.

Feature operation

No specific operating instructions are required to use this feature.

Collect Call Blocking(Brazil)

In Brazil an automatic long distance collect call service called DDC is available. The collect Call Blocking feature enables a Meridian 1 administrator to block DDC calls on incoming Direct Inward dialing (DID) and Public Exchange/Control Office trunks (analog or DT12). Under the following conditions, the Meridian 1 sends a special answer signal to the Central Office that collect calls cannot be accepted:

— The Collect Call Blocking (CCB) package 290 is enabled

— The incoming route has CCB enabled via the CCB prompt in the Route Data Block, and

— The call is answered by a CCB user (i.e., Collect Call Blocking Allowed Class of Service or option).

New Classes of Service and prompts have been introduced to inhibit specific users fro receiving collect DID and Central Office calls. These can be configured for the following:

— PBX and BCS through the Collect Call Blocking Allowed/Denied (CCBA/CCBD) Class of Service.

— Attendant and Network Alternate Route Selection calls on a per customer basis through CCBA/CCBD option.

— Automatic Call Distribution (ACD) queues through the CCBA prompt.

— Direct Inward system Access (DISA) through the CCBA prompt.

— Tandem calls dialed with Coordinated Dialing Plan (CDP) (Trunk Steering Code, Distant Steering Code) through the CCBA prompt.

— Tandem non-CDP calls through the CCBA prompt in the Route Data Block from the outgoing trunk route.

The Meridian 1 sends the CCB answer signal in place of the regular signal for incoming DID/CO calls from routes with CCB enabled, when a call is answered by a CCB user. If the call is a collect call, the CO will disconnect the call.

Operating parameters

The Collect Call Blocking feature supports both analog and DT12 trunks, and the following Intelligent Peripheral Equipment (IPE) cards:

— The NTCK 16BB Extended Flexible COT Trunk Card (XFCOT) with firmware flash timing

— The NT8D14BA Enhanced Extended Universal Trunk Card (EXUT) containing the Centrex Switchhook Flash function in the firmware, and

— The NT8K14AK Extended Universal Trunk Card (XUT) which may be used if the Centrex Switchhook Flash is configured with software timing.

— The Collect Call Blocking answer signal can only be sent in cases where answer supervision is provided by the Meridian 1.

Once the modified answer signal is sent to the CO, the Meridian 1 has no control over how the call will be handled by the CO.

If a CCB user answers a call from a CO/DID route with Collect Call Blocking activated, the CCB answer signal is sent to the CO for all incoming DID and CO calls. For analog trunks, the user will experience clicking on the line and a temporary break is speechpath (0.5 to 2.5 seconds) while the CCB answer signal is being sent.

If the XFCOT and EXUT cards do not have flexible firmware timing, the CCB flash portion of the CCB answer signal will be returned to the CO. However, software controlled signaling can be done with EXUT cards.

In a standalone environment, all input from a set (except from the Release key) is ignored while the Collect Call Blocking answer signal is being sent.

Collect Call Blocking is applied to attendants on a customer basis only; it cannot be applied on a tenant basis.

The answer signal returned for a call from a route with CCB enabled and that is Network Attendant Service (NAS) routed is determined by the customer option on the source node. Thus, NAS routing can be configured across any Meridian Customer Defined Network environment, but the source node determines the answer supervision sent to the CO.

Call Detail Recording (CDR) record timing begins on the first answer of the CCB answer sequence. For this reason, CDR records will be generated for incoming calls to CCB users across routes on which CCB is enabled. If the call is collect, and is dropped, a CDR record of approximately CCB1 + CCB2 length will be generated.

For data calls all calls will be answered with the CCB answer signal, if CCB is enabled. This may have an effect on data protocols, while CCB signaling is taking place.

If firmware timing is used (FWTM = YES in LD 14) for sending the CCB flash, the CCB2 timer is downloaded to the card before sending the firmware flash. If the CCB2 timer is changed in the Route Data Block, either the card has to be enabled or the switch has to be initialized to get the new CCB2 timer downloaded to the card.

Feature interactions

Automatic Answerback The Automatic Answerback (AAB) feature, when assigned to a BCS set, allows any incoming N) to be answered automatically. If an incoming DID or CO call terminates on a set with the AAB feature enabled, the call is automatically answered after one ring. If the set has a CCBA Class of Service, the CCB answer signal is provided in the place of the regular answer signal.

Automatic Call Distribution Collect Call Blocking can be enabled on an ACD queue basis. Hence, if an incoming CO or DID call is answered by an ACD agent, the answer supervision signal that is returned to the CO is determined by the value of the CCBA prompt in LD 23. While the CCB answer signal is being sent, the same limitations apply to ACD as apply to sets with CCBA Class of Service.

Automatic Call Distribution Interflow If an ACD call from a route with CCB enabled is diverted to an interflow DN, and answer supervision has not already been provided, the answer signal returned to the CO depends on the source ACD queue. The CCB answer signal is returned to the CO if the source ACD queue has CCB enabled.

Automatic Call Distribution Night Call Forward If an ACD call from a route with CCB enabled is diverted to a Night Call Forward DN, and answer supervision has not already been provided, the answer supervision signal returned to the CO depends on the source ACD queue. The CCB answer signal is returned to the CO if the source ACD queue has CCB enabled.

Automatic Call Distribution Night RAN Route Announcement If an ACD call from a route with CCB enabled is diverted to a Night RAN route (defined by NRRT in the ACD block), the CCB signal returned to the CO depends on the source ACD queue. If the source ACD queue has CCB enabled, the CCB answer signal is sent to the CO.

Autoterminate If an incoming DID or CO call from an autoterminate trunk terminates on a set or ACD queue with a CCBA Class of Service, the CCB answer signal is provided in place of the regular answer signal.

Basic Rate Interface (BRI) Sets

For BRI sets CCBA/CCBD Class of Service cannot be programmed. Therefore, it is not possible to prevent BRI sets from accepting DDC collect calls.

Central Answering Position (CAP) The answer signal returned to the CO for calls that get answered by a Central Answering Position (CAP) is determined by the source ACD configuration and not the customer option (CCBA/CCBD in LD 15) on the source node.

Centralized Attendant Service The answer signal returned to the CO for calls that get answered by a Centralized Attendant Service is determined by the customer option (CCBA/CCDB in LD 15) on the source node.

Centrex Switchhook Flash A Centrex Switchhook Flash cannot be invoked by another feature while the CCB answer signal is being sent.

Enhanced Malicious Call Trace If a station activates Malicious Call Trace (MCT) while the CCB answer signal is being sent, MCT activation is ignored. This also applies to the case when MCT is activated from a remote node.

Meridian Mail Because Meridian Mail is configured using ACD queues, the same interactions exist as in the ACD case. When Meridian Mail sends a call answer message to the Meridian 1, the CCB configuration in the source ACD queue is used to determine if a CCB answer signal should be sent to the Central Office. All mail boxes using the same ACD queue to access Meridian Mail will get the same CCB treatment.

If some of the mail boxes are allowed to receive collect calls, this may be a problem. A possible solution is to configure two ACD queues on the Meridian 1 to access Meridian Mail. One queue would have collect calls allowed (i.e.e, CCBA = NO) and the second queue would have collect calls denied (i.e.e, CCBA = YES).

Network Automatic Call Distribution The answer signal returned to the CO for a network ACD call from a route with CCB enabled is determined by the source ACD queue. If the source ACD queue has CCB enabled, the CCB answer signal is returned in place of the regular answer signal.

Pilot DN If an incoming DID or CO call has CCB enabled and is routed to a pilot DN, the answer signal returned to the CO is determined by the CCB configuration of the terminating station.

Private Line Service If an incoming DID or CO call from a private line trunk terminates on a set with a CCBA Class of Service, the CCB answer signal is provided in place of the regular answer signal.

Recorded Announcement (RAN) A RAN route is defined as having CCBA YES or NO, which is used if Coordinated Dialing Plan (CDP) or ACD queues were not used to get to the RAN route. If the call is routed through ACD/CDP to terminate on RAN, the CCB treatment will depend upon the CCB data of the ACD/CDP, and not the RAN route.

Tandem to Unsupervised Trunk If an incoming DID or CO call tandems to an unsupervised trunk before it terminates, the answer signal is sent by time-out. Therefore, any CCB tandem calls made to unsupervised trunks will not have the CCB answer signal sent until the time-out occurs.

Trunk Hook Flash (THF) If a station activates THF while the CCB answer signal is being sent, THF activation is ignored.

Feature packaging

Collect Call Blocking (CCB) package 290 must be provisioned to activate this feature.

Feature implementation

LD 16—Enable Collect Call Blocking on a route and configure timers. (Part 1 of 2)

REQ	NEW CHG	Add, or change.
TYPE	RDB	Route Data Block.
CUST	0-99	Customer number.
ROUT	0-511	Route Number.
TKTP	aaa	Trunk type. Must be COT,DID,FEX, or WAT for CCB.
...		
M911_ANI	NO	M911 route. Must be set to NO to enable CCB.
ISDN	NO	ISDN route. Must be set to NO to enable CCB.
...		
ICOD	IAO ICT OGT	Incoming and outgoing Incoming Outgoing Must be either IAO or ICT to enable CCB. Must be either IAO or OGT to get the CCBA prompt for outgoing calls.
...		
CNTL	(NO) YES	Collect Call Blocking enabled or disabled on incoming route. CCB package 290 is required. Enter YES to obtain CCB timer prompts.

LD 16—Enable Collect Call Blocking on a route and configure timers. (Part 2 of 2)

CCB1	512-(1536)-4992	Collect Call Blocking delay timer 1 in milliseconds. Input rounded to the next multiple of 128 milliseconds.
CCB2	500-(1520)-2550	Collect Call Blocking delay timer 2 in milliseconds. Input rounded to the next multiple of 10 milliseconds. If any CCB route members (trunks) are using firmware timing (FWTM = YES in LD 14), changes to the CCB2 timer value will not take effect until the new timer value is downloaded to the card. This can be done by enabling the card or initializing the switch.
CCBA	(NO) YES	Collect Call Blocking allowed or denied for outgoing route.

LD 14—Setup the firmware timing for XFCOT and EXUT cards.

REQ	NEW CHG	Add, or change.
TYPE	DID COT FEX WAT	Trunk Type.
TN	l s c u	Terminal Number.
	c u	Terminal Number for the Option 11.
XTRK	ECUT XCOT	Type of card.
FWTM	(NO) YES	Firmware timing for flash. Enter YES to enable firmware timing.
CUST	0-99	Customer number.
RTMB	xxx xxx	Trunk route and member number.
SUPN	YES	Answer supervision required.

LD 15—Add or change Collect Call Blocking for attendants.

REQ	NEW CHG	Add, or change.
TYPE	CDB	Customer Data Block.
CUST	0-99	Customer number.
...		
CAS	(NO) YES	Centralized Attendant Service.
OPT	(CCBD) CCBA	(Deny) allow Collect Call Blocking.

LD 10—Add or change Collect Call Blocking for PBX sets.

REQ	NEW CHG	Add, or change.
TYPE	500	Telephone type.
TN	l s c u	Terminal Number.
	c u	Terminal Number for the Option 11.
...		
CLS	(CCBD) CCBA	(Deny) allow Collect Call Blocking.

LD 11—Add or change Collect Call Blocking for BCS sets.

REQ	NEW CHG	Add, or change.
TYPE	aaaa	Telephone type, where: aaaa = SL1, 2006, 2008, 2009, 2016, 2018, 2112, 2216. 2317, 2616, or 3000.
TN	l s c u	Terminal Number.
	c u	Terminal Number for the Option 11.
...		
CLS	(CCBD) CCBA	(Deny) allow Collect Call Blocking.

LD 23—Enable Collect Call Blocking on ACD queues.

REQ	NEW CHG	Add, or change.
TYPE	ACD	ACD data block.
CUST	0-99	Customer number.
ACDN	xxxx	ACD Directory Number.
...		
CCBA	(NO) YES	(Deny) allow Collect Call Blocking.

LD 24—Enable Collect Call Blocking on DISA blocks.

REQ	NEW CHG	Add, or change.
TYPE	DIS	DISA data block.
CUST	0-99	Customer number.
...		
DN	xxxxxxx	DISA Director Number.
...		
CCBA	(NO) YES	(Deny) allow CCB answer signal to be sent.

LD 87—Enable Collect Call Blocking on CDP Steering codes.

REQ	NEW CHG	Add, or change.
CUST	0-99	Customer number.
FEAT	CDP	Coordinated Dialing Plan
TYPE	TSC DSC	Steering code type.
...		
CCBA	(NO) YES	(Deny) allow CCB answer signal to be sent.

Feature operation

No specific operating instructions are required to use this feature.

Direct Private Network Access

The Direct Private Network Access feature provides enhancements to the processing of Direct Inward System Access (DISA) and Authcode last request calls. This feature complements existing Meridian 1 capabilities to provide an arrangement suitable for long distance resellers. Typically, subscribers to these resellers" services dial in through a DISA port and require some automated digit manipulation, recorded announcements and Authcodes for billing purposes. This feature offers the following capabilities:

DISA Digit Insertion

Once a DISA Director Number (DN) is accessed, the Meridian 1 automatically inserts from 1 to 31 digits to save the caller from having to manually enter these digits. Dial tone is provided if the system expects to receive more digits from the caller in order to complete the call. If no additional digits are required, the call terminates automatically.

DISA Recorded Announcement (RAN)

A caller may be greeted with a Recorded Announcement once a DISA DN is accessed. The caller can begin dialing anytime during the greeting, in which case the greeting is stopped and the call is processed. If the Recorded Announcement finishes, dial tone is provided if more digits are expected from the caller to complete the call. As with the case of DISA Digit Insertion, the call terminates automatically if no additional digits are required.

Authcode Last Retry

For an Authcode last request call, if a caller enters an authorization code (Authcode) that is invalid, the caller is prompted to enter an Authcode again. The reprompt for the Authcode takes the form of either an Authcode Last Request dial tone or a RAN before the Authcode Last Request dial tone.

If configured, the RAN indicates to the caller that a wrong Authcode has been entered. While RAN is being given, all dialed digits are ignored.

If a caller realizes they have misdialed, an octothorpe (#) can be pressed which allows the user to immediately re-enter the Authcode. If an invalid Authcode is entered for a second time, the existing invalid Authcode treatment results.

Operating parameters

DISA Digit Insertion, DISA RAN, and Authcode Last Retry can be activated individually or can be combined to work in conjunction with one another.

ISA Digit Insertion and DISA RAN can be optionally assigned on a per DISA basis in LD 24, and are only applicable to DISA calls.

Authcode Last Retry can be optionally assigned on a per customer basis in LD 88, and is applicable to all call types supporting Authcode Last.

All existing DISA limitations apply to the DISA Digit Insertion and DISA RAN functionalities.

All existing RAN limitations apply tot he DISA RAN and Authcode Last Retry functionality.

All existing Authcode Last limitations apply to the Authcode Last Retry functionality.

To support DISA RAN and the Authcode Last Retry RAN function, the Meridian 1 must be equipped with all the necessary RAN hardware.

Feature interactions

Attendant Console Operation

Authcode Last Retry Not Configured

If an invalid Authcode is entered by an attendant, overflow tone is given as soon as a sufficient number of Authcode digits has been entered. If the attendant enters some digits from an Authcode that is less than the number of digits defined in LD 88, silence is heard.

Authcode Last Retry Configured

If the caller is an attendant and the Authcode entered is invalid, once a sufficient number of digits has been entered, the Authcode Last Request dial tone is immediately given to reprompt for the Authcode. If the attendant enters some digits for an Authcode that is less than the number of digits defined in LD 88, silence is heard. Since there is no interdigit time out for an Attendant Console, no Authcode Last Request dial tone will be given for retry.

Authcode Last Request tone will be heard immediately prompting for Authcode Retry if the attendant enters some digits and an octothorpe "#".

Autodial If Autodial is programmed with a valid Authcode for Authcode Last followed by an octothorpe "#", the existing Authcode Last operation will reject the Authcode as an invalid Authcode. If Authcode Last Retry is defined, the caller will be reprompted for the Authcode.

Call Detail Recording (CDR) Digits inserted by DISA Digit Insertion are reflected in the CDR record.

When a caller is reprompted for an Authcode due to Authcode Last Retry, and a new Authcode is entered, the second Authcode will overwrite the first entry. Therefore, the CDR record only reflects the last Authcode entered.

Pretranslation Digits automatically inserted by DISA Digit Insertion are pretranslated during call processing in the same manner s if the caller had manually dialed the digits.

Speed Call If a Speed Call entry is programmed with a valid Authcode for Authcode Last followed by an octothorpe "#", the existing Authcode Last operation will reject the Authcode as an invalid Authcode. If Authcode Last Retry is defined, the caller will be reprompted for the Authcode.

Feature packaging

This feature is packaged under Direct Private Network Access (DPNA) package 250.

DISA Digit Insertion requires the following additional package:

— Direct Inward system Access (DISA) package 22.

DUSA RAN requires the following additional packages:

— Direct Inward system Access (DISA) package 22, and

— Recorded Announcement (RAN) package 7.

Authcode Last Retry requires the following additional packages:

— Basic Authorization Code (BAUT) package 25

— Network Authorization Code (NAUT) package 63, and

— Recorded Announcement (RAN) package 7 when an Authcode Last Retry RAN is required.

Feature implementation

DISA DN Data Configure RAN routes (LD 16) and RAN trunks (LD 14) as per existing procedures.

LD 24—Respond as follows.

REQ	NEW CHG	New, or change.
TYPE	DIS	DISA data.
CUST	0-99	Customer Number.
...		
RANR	0-511	Route number for DISA RAN. The valid range of a route number for Option 11 is 0-127.
	(X)	Removes and deactivates DISA RAN>
-RTMR	10-300	The maximum amount of time (in seconds) that a caller can wait for an available RAN trunk before being removed from the RAN queue and proceeding as if DISA RAN has been completed.
	(0)	Removes and deactivates the timer.
DGTS	x...x	Digits for DISA Digit Insertion. Up to 31 digits can be defined.
	(X)	Removes and deactivates DISA Digit Insertion.
-DLTN	(YES)	Dial tone needed after digit insertion.
	NO	Dial tone not needed after digit insertion.

Authcode Data Configure RAN routes (LD16) and RAN trunks (LD 14) as per existing procedures.

LD 88—Respond to the following prompts.

REQ	NEW,CHG	New, or change.
TYPE	AUB	Authcode data.
CUST	0-99	Customer Number.
...		
RANR	0-511	Route number for Authcode Last Retry RAN.
RTRY	(NO)	Disable Authcode Last Retry.
	YES	Enable Authcode Last Retry.
-RAN2	0-511	Route number for Authcode Last Retry RAN. The valid range of a route number for Option 11 is 0-127.
	(X)	Removes and deactivates Authcode Last Retry RAN.
CLAS	xxx	Class code value assigned to authcode.

Feature operation

Operational Sequence of a DISA Call (Part 1 of 2)

Step	User Action	Result
1.	Dials DISA DN.	If DISA Security Access Code is required, special dial tone is given, and the caller continues to Step 2. Otherwise the caller skips to Step 3.
2.	Enters the Security Access Code	The dial tone is removed as soon as the first digit is dialed. If the security access code entered is valid, the caller continues to Step 3. Otherwise, the existing treatment for invalid Security Access code is given when the interdigit timer expires.
3.	<no user action>	If Authcode is required, normal dial tone is given, and the caller continues to Step 4. Otherwise, the caller skips to Step 5.

Operational Sequence of a DISA Call (Part 2 of 2)

Step	User Action	Result
4.	Enters an Authcode.	The dial tone is removed as soon as the first digit is dialed. If the Authcode entered is valid, the caller continues to Step 5. Otherwise, the existing invalid Authcode treatment is given when the interdigit timers times out.
5.	<no user action>	If DISA Digit Insertion is not configured, the caller immediately continues to Step 6. Otherwise, the digits defined for DISA Digit Insertion are automatically inserted into the call register before the caller continues to Step 6.
6.	<no user action>	If DISA RAN is configured, a RAN greeting is provided, and the caller continues to Step 7. Otherwise, the caller skips to Step 8.
7.	a) The caller listens to the RAN greeting; or	a) If DISA Digit Insertion is not defined, or DISA Digit Insertion specifies to give dial tone to prompt the caller to enter more digits, the caller continues to Step 8. Otherwise, the inserted digits are immediately processed for call completion.
	b) begins dialing before the RAN is finished	b) The RAN greeting is stopped as soon as the first digit is dialed. The dialed digits are appended into the call register (i.e., if DISA Digit Insertion is defined, the dialed digits are stored after the inserted digits), and the call is processed for call completion.
8.	<no user action>	Dial tone is given and the caller continues to Step 9.
9.	Dials digits to originate the call	Dial tone is removed as soon as the first digit is dialed. The dialed digits are appended into the call register (i.e., if DISA Digit Insertion is defined, the dialed digits are stored after the inserted digits), and the call is processed for call completion.

Operational Sequence of Authcode Last (Part 1 of 2)

Step	User Action	Result
1.	Makes an outgoing call that requires Authcode Lase.	Authcode Last Request dial tone is given. If Authcode Last RAN is defined, RAN precedes the dial tone. The caller continues to Step 2.
2.	Dials one of the following	The Authcode Last Request dial tone is removed as soon as the first digit is dialed. Then depending on the digit input, one of the following occurs:
	a) A valid Authcode.	a) The call is processed for call termination.
	b) An invalid Authcode followed by "#"	b) If Authcode Last Retry is defined, Authcode Last Request dial tone is immediately given (if Authcode Last Retry RAN is defined RAN precedes the dial tone), and the caller continues to Step 3. If Authcode Last Retry is not defined, when the interdigit timer expires the existing invalid Authcode treatment is given.
	c) An invalid Authcode	c) If Authcode Last Retry is defined: — If the caller is an attendant, Authcode Last Request dial tone is immediately given (if Authcode Last Retry RAN is defined RAN precedes the dial tone), and the caller continues to Step 3. — If the caller is not an attendant, when the interdigit timer expires Authcode Last Request dial tone is again given (if Authcode Last Retry RAN is defined RAN precedes the dial tone), and the caller continues to Step 3. If Authcode Last Retry is not defined, when the interdigit timer times out the existing invalid Authcode treatment is given.

Operational Sequence of Authcode Last (Part 2 of 2)

Step	User Action	Result
3.	dials one of the following	The Authcode Last Request dial tone is removed as soon as the first digit is dialed. Then depending on the digit input, one of the following occurs:
	a) A valid Authcode	a) The call is processed for call termination.
	b) An invalid Authcode followed by "#"	b) When the interdigit timer times out, the existing invalid Authcode treatment is given.
	c) An invalid Authcode.	c) When the interdigit timer times out, the existing invalid Authcode treatment is given.

Electronic Lock Network Wide/Electronic Lock on Private Lines

The basic Electronic Lock feature has been enhanced to provide the following capabilities:

— The feature can be implemented network wide.

— A new Class of Service, Controlled Network Class of Service (CNCS) can be selected in the Customer Data Block (LD 15).

— Locking can be implemented for Private DNs.

In a Meridian Customer Defined Network (MCDN) environment, Electronic Lock Network Wide can be used to change the Class of Service of a set in a remote location. Electronic Lock Network Wide is activated or deactivated from any node by dialing the electronic Lock Flexible Feature Code (FFC), a password, a location code, and the DN of the set to be changed. Since the password length defined at the destination node is not known at the originating node, the Station Control Password (SCPW) length (defined in LD 15) must be defined the same for all network nodes.

If the originating node has the FFC Confirmation Tone option selected, a confirmation tone is given when the feature is successfully activated or deactivated. Overflow tone is given if the operation is unsuccessful. There is no FFC verify code for Electronic Lock.

When a locked set makes an outgoing trunk call, if Controlled Network Class of Service is defined, the Network Class of Service (NCOS) defined by CNCS is used instead of the NCOS defined in LD 10 or 11 for the set. If network signaling is configured for the trunk that normally transmits the NCOS of the set between electronic Switched Network (ESN) nodes, the CNCS is transmitted instead of the NCOS. This prevents a locked set from reaching the exchange network by tandeming through a TIE trunk using ESN.

A new prompt (PELK) is introduced in the Customer Data Block to implement electronic Lock on private lines. If this option is enabled, an outgoing call on a private line of a locked set is subject to the same restrictions as all other DNs on the set. The same intercept treatment would be given as for a regular DN. The restrictions for private lines, as well as other DN keys on the set, are controlled by the Controlled Class of Service (CCOS), and by the CNCS if defined. Therefore, for outgoing calls, the Class of Service restrictions and/or New Flexible Code Restriction (NFCR) apply to private line keys on locked sets. Only outgoing calls are affected. The Class of Service of anon-locked set has no affect on private lines.

Operating parameters

The Network Dialing Plan must be either a coordinated Dialing Plan (CDP) or a Uniform Dialing Plan (UDP).

The set password lengths must be equal for all nodes in the network.

Network wide operation is only supported through an MCDN ISDN network.

The Electronic Lock feature must be equipped on both originating and remote nodes.

The FFC used is defined on the node from which Network Electronic Lock is being activated. To activate or deactivate Network Electronic Lock from any remote node, the user has to use the FFC Electronic Lock Activate (ELKA) or Electronic Lock Deactivate (ELKD) code defined on that remote node.

ISDN Basic Rate Interface (BRI) sets cannot be used to lock another set, nor can they be locked themselves.

A PBX (2500/500) set with a private line DN or a BCS set with a private line on the Prime DN cannot be locked.

The following hardware is required:

— Primary Rate Interface—D-channel Handler Interface (DCHI)/Multipurpose Serial Data Link (MSDL) and PRI/PRI12 cards.

— Integrated Services Digital Network Signaling Link (ISL)—DCHI cards and TIE trunks.

— Virtual Network Services (VNS)—DCHI cards and any trunks.

Feature interactions

Automatic Call distribution (ACD) An ACD set cannot be locked.

Call Forward (CFW) Call Forward No Answer (CFNA) For Call Forwarding, the COS and NCOS used for the forwarding call can be taken from either the forwarding set or from the forwarded set, depending on the option defined in the Customer Data Block.

For example, set B call forwards all calls to an external trunk. Set A calls set B. If OPT = CFF in LD 15 (Call Forward forwarded to party's COS and NCOS), the COS and NCOS of set B are used for forwarding the call to the trunk. If OPT = CFO (Call Forward originating party's COS and NCOS), the COS and NCOS of set A are used for forwarding the call to the trunk.

Direct Inward System Access (DISA) The Electronic Lock feature Cannot be activated or deactivated when accessing the node through DISA.

Digital Private Network Signaling System (DPNSS1) Digital Access Signalling system (DASS2) Analog Private Network Signalling System (APNSS) Electronic Lock Network Wide is not supported on DPNSS1, DASS2, or APNSS trunks.

Electronic Switched Network Authcode If a station user enters an authcode on the set, regardless of the status of the set being locked or not, the NCOS defined for the authcode is used. The ESN Authcode feature overrides the Electronic Lock Network Wide feature.

Flexible Numbering Plan If a network is equipped with a flexible numbering plan (i.e., not all the network DNs are the same length), handing up before the usual end-of-dialing timeout cancels the request for activation or deactivation of Electronic Lock. Dialing an octothorpe (#) after the network DN will cause the request for activation or deactivation of the electronic Lock to be sent immediately, instead of waiting for the usual end-of-dialing timeout to send it.

Multiple Appearance DN The same locked or unlocked state applies to all Terminal Numbers with the same primary DN and the same SCPW. Terminal Numbers with the same DN, but not having the same SCPW, cannot be locked or unlocked.

New Flexible code Restriction (NFCR) With NFCR, toll denied stations are allowed or denied calling privileges according to the Facility Restriction Level (FRL) assigned to the NCOS defined in the protected line block. For a locked set, NCFR uses the FRL assigned to the CNCS to determine its calling privileges if one is defined; if no CNCS is defined, the NCOS of the locked set will be used.

Scheduled Access Restrictions (SAR)

The SAR feature overrides Electronic Lock.

Virtual Network Services (VNS) Electronic Lock can function in a VNS environment.

Feature packaging

Electronic Lock Network Wide/Electronic Lock on Private Lines is packaged under Flexible Feature Codes (FFC) package 139.

Use of this feature requires the following additional packages:

— Controlled Class of Service (CCOS) package 81

— Network Class of Service (NCOS) package 32, and

— Integrated Services Digital Network (ISDN) package 145.

Feature implementation

Electronic Lock Network Wide/Electronic Lock on Private Lines is configured in the same way as Electronic Lock (currently described in the Flexible Feature Codes module of this document), except for the inclusion of the CNCS prompt in LD 15. In addition, to implement Electronic Lock on Private Lines, prompt PELK must be set to YES.

LD 15—Respond to the CNCS prompt as follows:

REQ	NEW CHG	New or change.
TYPE	CDB	Customer Data Block.
CCOS	YES	Change CCOS options.
SPRE	xxxx	Special Prefix number.
CCRS	(UNR),CUN,CTD,TLD, SRE,FRE,FR1,FR2	Controlled Class of Service.
CNCS	(X) 0-99	Controlled NCOS.
PELK	(NO) YES	Electronic Lock on Private Lines.
SCPL	(0)-8	Station Control Password length.

Feature operation

Electronic Lock Network Wide N ISDN network is set up connecting Node 1 to Node 2. Set A is the Controlling set. Set B is the set to be locked and unlocked by Set A. The digits that set A would dial to ring set B are to be in the format of a CDP or UDP dialing plan. This is standard dialing for ISDN features.

To lock set B (in Node 1) from set A (in Node 2), the user goes off-hook and dials the electronic Lock Activate (ELKA) FFC defined in the Customer Data Block of Node 1, followed by the Station Password (SCPW) defined for set B, and the digits that set A would normally dial to ring set B (e.g., 41 + 9999 + 6-343-3000). If the FFCT option is configured as YES in LD 57 in the Customer Data Block of Node 1, confirmation tone is given to set A to confirm that the lock operation has been successful. Set B becomes locked if it was previously in an unlocked state.

If set B was already locked, the above operation is ignored and Set B remains locked; however, a confirmation tone is provided to verify that the set is locked.

If the lock operation was unsuccessful, overflow tone is given.

To unlock set B (in Node 1) from set A (in Node 2), the user goes off-hook and dials the Electronic Lock Deactivate (ELKD) FFC defined in the Customer Data Block of Node 1, followed by the SCPW defined for set B and the digits that set A would normally dial to ring set B (e.g., 42 + 9999 + 6-343-3000). If the FFCT option is configured as YES in LD 57 in the Customer Data Block of Node 1, confirmation tone is given to set A to confirm that the unlock operation has been successful. Set B becomes unlocked it is was previously in a locked state.

If Set B was already unlocked, the above operation is ignored and Station B remains unlocked; however, a confirmation tone is provided to verify that the set is unlocked.

If the unlock operation was unsuccessful, overflow tone is given.

Electronic Lock on Private Lines Feature operation of Electronic Lock for Private Lines is the same as for the basic Electronic Lock feature.

Controlled Network Class of Service No specific operating instructions are required to use Controlled Network Class of Service.

Three-Wire Analog Trunk - Commonwealth of Independent States (CIS)

The Three Wire Analog Trunk - Commonwealth of Independent States (CIS) feature provides the connectivity between the Meridian 1 and the three-wire analog trunks (3WT) used in the CIS. Analog incoming local three-wire trunks, analog incoming toll three-wire trunks, and analog outgoing Direct Inward Dialing (DID) three-wire trunks can be connected to the Meridian 1.

The following hardware cards are supported:

— Cards supported in an Enhanced Peripheral Equipment (EPE) environment are referred to as E3W cards. They consist of:

- APC661 for incoming trunk calls.
- QPC661 for incoming toll calls.
- QPC661 for outgoing 3WT local trunks.

— Cards supported in an Intelligent Peripheral Equipment (IPE) environment are referred to as X3W cards. They consist of:

- NT5K60AA for incoming local and toll trunks
- NT5K61AA for outgoing trunks.

The following functions are provided by the Three-Wire Analog Trunk - CIS feature:

— Delivery of Automatic Number Identification (ANI) on request from the Public Exchange/Central Office for outgoing 3WT analog calls

— Downloading of specific transmission parameters (i.e., pad data, public network toll access code, and hardware ID) for X3W cards, and

— Provision of dial tone internally by the Meridian 1 to the originator of the call after seizure of an outgoing X3W trunk.

The trunk state change validation timing is performed by the 3WT cards. For 2WT trunks, the originating party controls the disconnection of a call. When the originating party goes on-hook, the call is released. Note however, that when Malicious Call Trace is enabled, the Local Exchange may require a two-way release. This two-way release applies only on a set.

A 3WT Unproductive Timer is used to prevent a call on a X3W trunk from remaining unanswered for too long. This timer can be set to a maximum of 10 minutes.

For outgoing calls, digits are sent from the main Central Processing Unit (CPU) to the 2WT firmware. This is done by Dual-tone Multifrequency (DTMF) signaling for E3W equipment, and by IPE messaging for X3W equipment. The firmware then sends the digits as pulses and controls the actual decadic outpulsing.

Digits for incoming calls are received by the 3WT firmware as pulses. For E3W equipment, each valid pulse is reported to the main CPU by Scan and Signaling Distributor (SSD) messages. For X3W equipment, the pulses are collected by firmware and complete digits are reported to the CPU as IPE digit messages.

Operating parameters

X3W trunk cards can only be configured on IPE shelves; E3W trunk cards can only be configured on EPE shelves.

Trunk-to-trunk connections are supported, but the ANI information will refer to the ANI DN of the incoming route, except with QSIG, Q931, and Digital Private Signaling System #1 (DPNSS1) routes. QSIG, and Q931 ANI information will use the Calling Line Identification (CLID) information, whereas DPNSS1 ANI will use the Originating Line Identifier (OLI) information if this information is present.

The Dynamic Loss Switching feature is not supported, because there is no connection matrix and loss alternative table available for the CID market. However, Dynamic Loss Switching is supported in Australia, New Zealand, Italy, and China.

The static Loss Plan Download (SLPD) feature is supported on X3W trunks.

No loss downloading/switching is done for E3W trunks.

ANI is only supported for outgoing calls.

The data in ANI is built only once at the beginning of the call. Once the trunk access code is dialed, the ANI information is downloaded to the 3WT firmware. The download of ANI occurs only once and is not changed or redownloaded for any kind of operation during a call; therefore, if the call goes through any type of modification such as a transfer or call forward for instance, the ANI information sent when requested is that of the original originator of the call.

Toll Operator Manual Ringing and Break-In are not supported on IPE analog trunks.

Data calls are supported, but with the limitations due to the 500 Hz ANI requests that can happen any time during the call and the ANI information being sent of the same voice circuit on which the data is being transmitted; therefore, the transmission of data is not guaranteed.

Multifrequency Shuttle signaling is not supported on either X3W or E3W trunk cards.

EPE interfaces cannot be used on the Option 11.

The CIS A-law XCT (NTD17AE) is required.

Feature interactions

Authorization Code An extension may, referring to the Authorization Code, seize an outgoing CIS 3WT trunk. The Authorization Code category is used to build the ANI message, meaning that a set which has a CIS restricting call category can complete a call to the public network using the Authorization Code.

Autodial Autodial on a E3W trunk will fail for toll calls. The reason is that E3W trunks do not wait for the ANI request from the Public Exchange/Central Office, which is expected to appear after the toll access code is dialed. The Public Exchange then does not accept the call due to failure to receive ANI information.

Dial Tone Detection Dial Tone detectors are supported with the limitations of the reliability of the tone provided by the Public Exchange.

DPNSS1 Gateway The ANI information transmitted for this incoming DPNSS1 route will include the Local Exchange Code (LEC) of the CIS outgoing route, the ANI DN, and the Category Code (CAC) of this incoming route.

The ANI DN information which is built will refer to the Originating Line Identifier (OLI) if present and the Route DN Length prompt for ANI (RDNL 0) in LD 16. If the OLI is available, but RDNL = 0 for that route, the ANI DN is the ANI DN of that incoming route. If the OLI is available, but RDNL = 0 and the ANI DN of the incoming route is not defined, the ANI DN is the ANI DN of the CIS outgoing route. If the OLI is available, but RDNL = 0, and the ANI DN of the incoming route is not defined, and the ANI DN of the CIS outgoing route is not defined, the ANI DN will be built with the Additional Digit (ADDG). If RDNL 0, its value will be the number of digits extracted from the OLI to be used as the ANI DN. The least significant digit of the OLI will be extracted (e.g., if the DN is 4201, the 1 is the least significant digit).

If there is no OLI, the ANI DN of the SPNSS1 route is used to build the ANI message. If there is no ANI DN on the DPNSS1 route, the ANI DN of the CIS outgoing route is used to build the ANI message. If there is no ANI DN on the CIS outgoing route, the ANI is built with the ADDGs of the CIS route (ADDG is always defined).

Incoming Digit Conversion The construction of an ANI message does not care if Incoming Digits Conversion is used. THe DN sent as ANI is the actual DN of the set, not necessarily the DID number of dial to reach the set. Therefore, if an external party uses a DN for making a call to the corresponding extension which is delivered in an ANI message, the call may fail.

Last Number Redial Last Number Redial on an E3W trunk will fail for toll calls. The reason is that E3W trunks doe not wait for the ANI request from the Public Exchange, that is expected to appear after the toll access code is dialed. The Public Exchange will not accept the call due to the failure to receive ANI information.

Multiple Appearance DNs Since the ANI category is defined on a per set basis, two stations with the same multiple Appearance DN can be assigned different ANI categories.

Q931 Gateway/BR1 Gateway The ANI information transmitted for this incoming Q931 route will include the LEC of the CIS outgoing route, the ANI DN, and the CAC of this incoming route.

The ANI DN information which is built will refer to the Calling Line Identification (CLID) if present and the Route DN Length prompt for ANI (RDNL 0) in LD 16. If the CLID is available but RDNL = 0 for that route, the ANI DN is the ANI DN of that incoming route. If the CLID is available, but RDNL = 0, and the ANI DN of the incoming route is not defined, the ANI DN is the ANI DN of the CIS outgoing route. If the CLID is available, but RDNL = 0, and the ANI DN of the incoming route is not defined, and the ANI DN of the CIS outgoing route is not defined, the ANI DN will be built with the ADDG. If RDNL 0), its value will be the number of digits extracted from the CLID to be used as the ANI DN. The least significant digits of the CLID will be extracted (e.g., if the DN is 4201, the 1 is the least significant digit).

If there is no CLID, the ANI DN of the Q931 route is used to build the ANI message. If there is no ANI DN on the Q931 route, the ANI DN of the CIS outgoing route is used to build the ANI message. If there is no ANI DN on the CIS outgoing route, the ANI is built with the ADDG of the CIS outgoing route (ADDG is always defined).

QSIG Gateway The ANI information transmitted for this incoming QSIG route will include the LEC of the CIS outgoing route, the ANI DN, and the CAC of this incoming route.

The ANI DN information which is built will refer to the Calling Line Identification (CLID) if present and the Route DN Length prompt for ANI (RDNL 0) in LD 16. If the CLID is available but RDNL = 0 for that route, the ANI DN is the ANI DN of that incoming route. If the CLID is available, but RDNL = 0, and the ANI DN of the incoming route is not defined, the ANI DN is the ANI DN of the CIS outgoing route. If the CLID is available, but RDNL = 0, and the ANI DN of the incoming route is not defined, and the ANI DN of the CIS outgoing route is not defined, the ANI DN will be built with the ADDG. If RDNL 0), its value will be the number of digits extracted from the CLID to be used as the ANI DN. The least significant digits of the CLID will be extracted (e.g., if the DN is 4201, the 1 is the least significant digit).

If there is no CLID, the ANI DN of the QSIG route is used to build the ANI message. If there is no ANI DN on the QSIG route, the ANI DN of the CID outgoing route is used to build the ANI message. If there is no ANI DN of the CIS outgoing route, the ANI is built with the ADDG digits of the CIS outgoing route (ADDG is always defined).

The ANI information transmitted for this incoming QSIG route will include the LEC of the CIS outgoing route, the ANI DN, and the CAC of this incoming route.

R2MFC Calling Number Identification The incoming R2MFC CNI will not be tandemed if the call is outgoing to a CIS trunk. The ANI built will be the LEC of the outgoing CIS route, the ANI DN of this R2MFC incoming route if defined (otherwise it will be the ANI DN of the outgoing CIS route, or the ADDG digit), and the CAC of the incoming R2MFC route.

The category (CAC) used to build and the R2MFC Calling Number Identification (CNI) for the analog, digital and Basic Rate Interface (BRI) sets is used to build the CIS ANI. The meaning of CAC is different between the R2MFC CNI signaling and the CIS signaling (analog BRI, and digital). R2MFC CAC prompt values are in the range of 0 to 10, and the default is 0. CIS CAC prompt values are in the range of 0 to 9, and the default value is 3.

If the MFC package is equipped, but not the CIST package, the CAC prompt uses the R2MFC range and default. If the CIST package is equipped (MFC package equipped or not), the CAC prompt uses the CIS range and default.

Speed Call Speed Call of the E3W trunk will fail for roll calls. E3W trunks do not wait for the ANI request from the Public Exchange, that is expected to appear after the toll access code is dialed. The Public Exchange will not accept the call due to the failure to receive ANI information.

Virtual Network Services Virtual Network Services is not supported on CIS trunks.

Feature packaging

The Three-Wire Analog Trunk - CIS feature is contained in Commonwealth of Independent States Trunk Interface (CIST) package 221.

The following packages are also required to implement this feature:

— Fast Tone and Digit Switch (FTDS) package 87 (only for E3W cards)

— Flexible Tones and Cadences (FTC) package 125

— International supplementary Features (SUPP) package 131 for DID/DOD

— Flexible Numbering Plan (FNP) package 160

— Trunk Failure Monitor (TFM) package 182, and

— Meridian 1 Extended Peripheral Equipment (XPE) package 203 (only for X3W cards).

Feature implementation

This is an example that describes how the 3WT related features are configured. Only the prompts that are significant for the Three-Wire Analog Trunk - CIS feature are mentioned.

The following features are needed to make the feature work according to this example: B34 Codec Static Loss Plan Downloading; Partial Dial Timer; End-of-Selection Busy; Tone to-Last Party; Special Dial Tones After Dialed Numbers; Trunk Barring, and Special Service List.

LD 17—Configure the system data.

REQ	NEW CHG	Add or Change.
...		
PARM	YES	Change system parameters.
PCML	A	System Pulse Code Modulation companding law. A-law is used to the CIS market.
...		
DTRB	70	Dual-tone Multifrequency burst and interdigit pause for the Tone and Digit Switch. Pulse/Pause Ration 70/70. For outgoing E3W cards, the preferable digitone burst time is 70 ms.

LD 16—Configure an incoming X3W DID route. (Part 1 of 2)

REQ	NEW CHG	Add, or change.]
TYPE	RDB	Route Data Block.
...		
TKTP	DID	Direct Inward Dialing trunk data block.
...		
DTRK	NO	This is not a digital trunk route.
...		
ICOG	ICT	Incoming trunk.
...		
CNTL	YES	Change control or timers.
- TIMR	ICF 0	Incoming flash timer should be set to 0. Validation is performed by 3WT firmware.
- TIMR	OGF 0	Outgoing flash timer should be set to 0. Validation has already been done by 3WT firmware.
- TIMR	EOD 13952	End of dial timer, default value in milliseconds.
- TIME	DSI 11904	Disconnect supervision timer in milliseconds.
- TIMR	DDL 0	Delay Dial Timer not needed.
...		
NEDC	ORG	Near End Disconnect Control. Originating end control.
CDPC	(NO)	Meridian 1 is not the controlling party on incoming calls.
...		

LD 16—Configure an incoming X3W DID route. (Part 2 of 2)

OPR	(NO)	This is not an outpulsing route.
PRDL	YES	Partial dial timing is equipped using EOD.
EOS	BSY	Busy signal is sent on time-out.
DNSZ	(0)-7	Number of digits expected on DID routes. 0, the default, indicates no fixed value. This value must be defined according to the numbering plan.
...		
BTT	30	Busy Tone Time. Length of Busy/overflow to be returned on DID routes in seconds.
...		
CAC	0-(3)-9	Route ANI category.
ANDN	0-9999999	Route ANI DN.
RDNL	0-(4)-7	Route DN Length for ANI. This is printed for DPNSS1, MCDN, and QSIG routes only.

LD 16—Configure an outgoing X3W DID route and define the toll digit using the TDG prompt. (Part 1 of 2)

REQ	NEW CHG	Add, or change.
TYPE	RDB	Route Data Block.
...		
TKTP	DID	direct Inward Dialing trunk data block.
...		
DTRK	NO	This is not a digital trunk route.
...		
ICOG	OGT	Outgoing trunk.
...		
CNTL	YES	Change control or timers.
- TIMR	ICF 0	Incoming flash timer should be set to 0 in milliseconds. Validation will be done by 3WT firmware.
- TIMR	OGF 0	Outgoing flash timer should be set to 0 in milliseconds. Validation will be done by 3WT firmware.
- TIMR	EOD 13952	End of dial timer, default value.
- TIMR	DSI 11904	Disconnect supervision timer.
- TIMR	DDL 0	Delay Dial Timer not needed.
- TIMR	GTO 2944	Outgoing guard timer.
...		
NEDC	ETH	Near End Disconnect Control Either end control.
FEDC	ETH	Far End Disconnect Control Either end control.
...		
NATL	NO	North American Toll scheme.
TDG	8	Toll Digits. List of digits after trunk access code which indicate toll calls.

LD 16—Configure an outgoing X3W DID route and define the toll digit using the TDG prompt. (Part 2 of 2)

...		
OPR	(NO)	This is not an outpulsing route.
...		
ADKW	(NO)	Seizure acknowledge signal is not expected.
...		
LEC	0-9999999	Local Exchange Code. A value must be entered.
ADDG	0-(8)-9	Additional digit.
CAC	0-(3)-9	Route ANI category.
ANDN	0-9999999	Route ANI DN.
RDNL	0-(4)-7	Route DN Length for ANI. This is printed for DPNSS1, MCDN, and QSIG routes only.

LD 18—Configure the Special Service List.

REQ	NEW CHG	Add, or change.
TYPE	SSL	Special Service List data block.
CUST	0-99	Customer number.
SSL	1-15	List number for Special Service List.
SSDG	xxxx	Special Service Digit or Digits (1 to 4 digits).
...		
- TOLL	YES	The SSDG entry is a toll number.
...		
SSDG	xxxx	Special Service Digit or Digits (1 to 4 digits).
...		
- SSUC	YES	The SSDG entry is a Special Service unanswered call.
SSDG	<CR>	

LD 16—Configure an outgoing X3W DID route and define the toll access code using the SSL prompt. (Part 1 of 3)

REQ	NEW, CHNG	Add, or change.
TYPE	RDB	Route Data Block.
...		
TKTP	DID	Direct Inward Dialing trunk data block.
...		
DTRK	NO	This is not a digital trunk route.
...		
ICOG	ICT	Incoming trunk.
...		
CNTL	YES	Change control or timers.

LD 16—Configure an outgoing X3W DID route and define the toll access code using the SSL prompt. (Part 2 of 3)

- TIMR	ICF 0	Incoming flash timer should be set to 0. Validation has already been done by 3WT firmware.
- TIMR	OGF 0	Outgoing flash timer should be set to 0. Validation has already been done by 3WT firmware.
- TIMR	EOD 13952	End of dial timer, default value.
- TIMR	DSI 11904	Disconnect supervision timer.
- TIMR	DDL 0	Delay Dial Timer not needed.
...		
NEDC	ORG	Near End Disconnect Control Originating end control.
FEDC	ORG	Far End Disconnect Control Originating end control.
CDPC	(NO)	Meridian 1 is not the controlling party on incoming calls.
...		
OPR	(NO)	This is not an outpulsing route.
PRDL	YES	Partial dial timing is equipped using EOD.
EOS	BSY	End of selection and busy signals enabled.
DNSZ	(0)-7	Number of digits expected on DID routes. 0, the default, indicates no fixed value. This value must be defined according to the numbering plan.
...		
BTT	30	Length of busy/overflow tone to be returned on DID routes in seconds.
...		

LD 16—Configure an outgoing X3W DID route and define the toll access code using the SSL prompt. (Part 3 of 3)

CAC	0-(3)-9	Route ANI category.
ANDN	0-9999999	Route ANI DN.
RDNL	0-(4)-7	Route DN Length for ANI. This is printed for DPNSS1, MCDN, and QSIG routes only.

LD 16—Configure an outgoing E3W COT route. (Part 1 of 2)

REQ	NEW CHG	Add, or change.
TYPE	RDB	Route Data Block.
...		
TKTP	COT	Central Office Trunk data block.
...		
DTRK	NO	This is not a digital trunk route.
...		
ICOG	OGT	Outgoing trunk.
...		
CNTL	YES	Change control or timers.
- TIMR	ICF 0	Incoming flash timer should be set to 0 in milliseconds. Validation will be done by 3WT firmware.
- TIMR	OGF 0	Outgoing flash timer should be set to 0 in milliseconds. Validation will be done by 3WT firmware.
- TIMR	EOD 13952	End of dial timer, default value.
- TIMR	DSI 11904	Disconnect supervision timer.
- TIMR	DDL 0	Delay Dial Timer not needed.
- TIMR	GTO 2944	Outgoing Guard Timer.
...		

LD 16—Configure an outgoing E3W COT route. (Part 2 of 2)

NEDC	ETH	Near End Disconnect Control Either end control.
FEDC	ETH	Far End Disconnect Control Either end control.
CDPC	(NO)	Meridian 1 is not the controlling party on incoming calls.
...		
NATL	NO	North American Toll scheme.
...		
LEC	0-9999999	Local Exchange Code.
ADDG	0-(8)-9	Additional digit.
CAC	0-(3)-9	Route ANI category.
ANDN	0-9999999	Route ANI DN.
RDNL	0-(4)-7	Route DN Length for ANI. This is printed for DPNSS1, MCDN, and QSIG routes only.

LD 14—Add or change trunk data for X3W incoming DID trunk.

REQ	NEW CHG	Add, or change.
TYPE	DID	Direct Inward Dial trunk data block.
...		
XTRK	XDID	Extended Trunk Type. IPE DID trunk card.
...		
SIGL	CIS	Trunk Signaling. Three-wire CIS trunk signaling.
CIST	(NO) YES	Prompted only for incoming routes (i.e., ICOG = ICT). NO = Local trunk. YES = Toll trunk.
...		
STRI	IMM	Immediate incoming start arrangement.
...		
SUPN	YES	Answer and disconnect supervision required.
CLS	(DIP)	Dial pulse (for 3WT incoming and outgoing).
	(SHL) LOL	Line length used for pad setting.
	(BARD) BARA	Barring (denied) allowed.

LD 14—Add or change trunk data for X3W outgoing DID trunk.

REQ	NEW CHG	Add, or change.
TYPE	DID	Direct Inward Dial trunk data block.
...		
XTRK	XDID	IPE DID trunk card.
...		
SIGL	CIS	Three-wire CIS trunk signaling.
...		
STRO	IMM	Immediate outgoing start arrangement.
...		
SUPN	YES	Answer and disconnect supervision required.
CLS	(DIP)	Dial pulse (for 3WT incoming and outgoing).
	(SHL) LOL	Line length used for pad setting.
	(BARD) BARA	Barring (denied) allowed.

LD 14—Add or change trunk data for E3W incoming three-wire trunk.

REQ	NEW CHG	Add, or change.
TYPE	DID	Direct Inward Dialing trunk data block.
...		
SIGL	EAM	Ear and mouth.
CDEN	DD	Double Density.
...		
STRI	IMM	Immediate incoming start arrangement.
...		
SUPN	YES	Answer and disconnect supervision required.
CLS	(DIP)	Dial pulse.

LD 14—Add or change trunk data for E3W outgoing three-wire trunk.

REQ	NEW CHG	Add, or change.
TYPE	COT	Central Office Trunk data block.
...		
SIGL	LOP	Loop start.
CDEN	DD	Double density.
...		
SUPN	YES	Answer and disconnect supervision required.
- STYP	PSP	Polarity sensitive care.
...		
SEIZ	YES	Answer and disconnect supervision required.
CLS	DTN	Digitone.

LD 10—Add or change PBX telephones for CIS.

REQ	NEW CHG	Add, or change.
TYPE	500	PBX (500/2500) telephone data block.
...		
CLS	(DNAA) DNAD	DN of set (allowed) denied for use in ANI messages.
CAC	0-9	Specifies ANI category for 3WT calls.

LD 11—Add or change BSC telephones for CIS.

REQ	NEW CHG	Add, or change.
TYPE	aaaa	Telephone type, where: aaaa = SL1, 2006, 2008, 2009, 2016, 2018, 2112, 2216, 2317, 2616, or 3000.
...		
CLS	(DNAA) DNAD	DN of set (allowed) denied for use in ANI messages.
CAC	0-9	Specified ANI category for 3WT calls.

LD 12—Add or change an Attendant Console for CIS.

REQ	NEW CHG	Add, or change.
TYPE	ATT 1250 2250	Console type.
....		
CLS	(DNAA) DNAD	DN of set (allowed) denied for use in ANI messages.
CAC	0-9	Specifies ANI category for 3WT calls.

LD 27—Add or change BRI sets for CIS.

REQ	NEW CHG	Add, or change.
TYPE	DSL	Digital Subscriber Loop data block.
...		
CLS	(DNAA) DNAD	DN of set (allowed) denied for use in ANI messages.
CAC	0-9	Specifies ANI category for 3WT calls.

LD 56—Configure dial tone, busy tone, and tone to last party. (Part 1 of 3)

REQ	NEW CHG PRT	Add, change, or print.
TYPE	MCAD	Master Cadence data block.
WACD	30	Cadence number. In this example entry 30 is modified.
CDNC	60 60	On-off phases for cadence.
REQ	NEW CHG PRT	Add, change, or print.
TYPE	FCAD	Firmware Cadence data block.
WACD	30	Cadence number. In this example entry 30 is modified.
CDNC	60 60	On-off phases for cadence. 0.3 second on. 0.3 second off.
END	REPT	Repeating cycles.
- CYCS	1	On/off cycles to be repeated.
- WTON	YES	Define tones associated with the cadence.
- - TONES	158	420 Hz and - 12 dB below overload.
REQ	NEW CHG PRT	Add, change, or print.
TYPE	FTC	Flexible Tones and Cadence data block. Used to provide special dial tone after dialed number.

LD 56—Configure dial tone, busy tone, and tone to last party. (Part 2 of 3)

...		
HCCT	YES	Hardware Controlled Cadences and Tones modification of the hardware.
...		
- BUSY		Busy tone.
- - TDSH		
- - XTON	158	420 Hz and - 12 dB below overload.
- - XCAD	30	XCT cadence number. 0.3 seconds on, 0.3 seconds off.
...		
- TLP		Tone to last party.
-- TDSH		
- - XTON	158	420 Hz and - 12 dB below overload.
- - XCAD	30	XCT cadence number. 0.3 seconds on, 0.3 seconds off.
- TLTP	30	Tone to last party timer in seconds.
...		
SRC	YES	Source Tones.
- SRC1		CIS continuous dial tone within the range.
- - TDSH		
- - XTON	158	420 Hz and - 12 dB below overload.
- - XCAD	0	No cadence.
REQ	NEW CHG PRT	Add, change, or print.

LD 56—Configure dial tone, busy tone, and tone to last party. (Part 3 of 3)

TYPE	DTAD	Special Dial Tone After Dialed Number data block.
DDGT	9	The digit 9 is to be used as an outgoing local access code.
TONE	SRC1	Tone to be provided after the dialed digit 9.

LD 88—Configure the Authcode data block.

REQ	NEW CHG	Add, or change.
TYPE	AUB	Authcode data block.
...		
CLAS	(0)-115	Classcode value assigned to Authcode (NAUT).
...		
NCOS	(0)-99	Network Class of Service Group number
CAC	0-9	specifies ANI category for CIS calls.

LD 97—Configure the IPE system record for three-wire trunks.

REQ	CHG	Change.
TYPE	LOSP	Loss Plan Tables. Configure loss parameters for downloading.
...		
TTYP	(STAT)	Install a B34 Static Los Plan Table.
- STYP	(PRED)	A numbered predefined table is to be used.
- - TNUM	2	2 = Austrian Table.
REQ	CHG	Change.
TYPE	LOSP	Los Plan Tables. Configure loss parameters for downloading.
...		
TTYP	(STAT)	Install a B34 Static Loss Plan Table.
- STYP	CSTM	Customize a numbered predefined table.
PWD2	xxxx	Response CSTM at STYP prompt requires a PWD2 password or a LAPW password with Loss Planning Customizing Allowed (LOSA) access. This prompt appears if the appropriate password has not been given previously.
-DIDS	Rx Tx	Enter loss levels for DID short line.
- DIDL	Rx Tx	Enter loss levels for DID long line.

Feature operation

No specific operating instructions are required to use this feature.

Authorization code administration

Classcodes

With the NAUT and BAUT features, a "classcode" structure is part of authorization code administration. A classcode is a combination of COS, TGAR, and NCOS codes. There can be up to 116 (0–115) classcodes defined through the Authorization Code Data Block (AUB, LD 88), each with a different combination of COS, TGAR, and NCOS codes. Authorization codes that have the same combination of COS, TGAR, and NCOS codes are assigned the same classcode.

Creating authorization codes

When creating new authorization codes, a classcode associated with the new authorization codes is specified. The new authorization codes will then be automatically assigned the COS, TGAR, and NCOS codes associated with the specified classcode.

> ***Note:*** The BAUT feature does not support automatic generation of authorization codes. With the NAUT feature, authorization codes can be defined individually by the customer or generated automatically by the Meridian 1.

Exemptcode

When an authorization code is to be removed from use, a facility exists to prevent that authorization code from being reused (that is, the authorization code will not be accepted as valid input when individually defining authorization codes). This is accomplished through an "exemptcode." When an authorization code is removed from use, an exemptcode is assigned to the authorization code in place of the classcode. The exemptcode is the month (for example, JAN, FEB) taken from the system clock. If an exemptcode is not requested, the removed authorization code is returned to the pool of unused authorization codes and can be reused at any time.

Default Facility Restriction Level

The Route List Block (RLB) program (LD 86) is used to define a minimum Facility Restriction Level (FRL) for each route list. This minimum FRL (range 0-7) is used to determine whether or not to prompt for an authorization code entry after a call. If a minimum FRL is not specified, the actual minimum FRL in the initial route set is used as a default. Similarly, the Route Data Block (RDB) program (LD 16) is used to define whether to prompt for an authorization code entry on calls on incoming or two-way tie trunk groups.

Network Authorization Code

The Network Authorization Code (NAUT) feature provides for up to 20,000 authorization codes of 1 to 7 digits.

> ***Note:*** With X11 release 13 and later, the authorization codes can be of 1 to 14 digits.

The NAUT feature incorporates all the features of the BAUT feature, adding two enhancements:

— a "conditionally last" option for entering an authorization code after dialing a NARS, BARS, or CDP call

— allowing the attendant to enter an authorization code

Authorization code conditionally last

With the NAUT feature, users can be prompted "conditionally" for an authorization code after dialing a NARS, BARS, or CDP call. The prompt is by an "authorization code request tone," which consists of 10 bursts of dial tone, followed by steady dial tone. (The authorization code request tone can, optionally, be preceded with an appropriate recorded announcement.) The user is prompted for an authorization code entry only if

— an authorization code was not previously entered

— the Facility Restriction Level (FRL) associated with the user's Network Class of Service (NCOS) is less than the service change assigned minimum FRL of the route list that NARS, BARS, or CDP would use for the call

Users at a remote switch (Meridian 1 Main or Conventional Main) connected via tie trunks to a Meridian 1 Node can (optionally) be prompted for an authorization code entry after dialing a NARS, BARS, or CDP call. The user is prompted for an authorization code entry only if

— an authorization code was not previously entered

— the FRL associated with the NCOS of the incoming (or two-way) tie trunk is less than the minimum FRL of the route list that NARS, BARS, or CDP would use for the call

— the route is defined in the Route Data Block (RDB), LD 16, to prompt for an authorization code entry on incoming NARS, BARS, or CDP calls

Users accessing a Meridian 1 Node via the Direct Inward System Access (DISA) feature to make a NARS, BARS, or CDP call are prompted for an authorization code entry only if

— an authorization code was not previously entered

— the FRL of the NCOS assigned to the DISA Directory Number (DN) is less than the minimum FRL of the route list that NARS, BARS, or CDP would use for the call

Attendant input of authorization code

Normally, because an attendant is not restricted from accessing any system resource, there is no need for the attendant to have an authorization code. The Network Authorization Code feature enables the attendant to enter an authorization code for other callers. For example, the attendant can enter an authorization code (after dialing the SPRE and the digit "6") and complete a long distance call for a local station user whose COS is toll denied (TLD). If the Call Detail Recording (CDR) of authorization codes is defined for the customer, the local station user's authorization code digits appear in the CDR record for billing purposes.

Attendants are normally assigned an NCOS having a high FRL so that they can make any type of call, including NARS, BARS, or CDP calls. An attendant can, however, be prompted for an authorization code entry if the FRL required to access a route list for a NARS, BARS, or CDP call is greater than the FRL of the attendant's NCOS.

Operating parameters

Users on PBX or Centrex systems connected via tie trunks to a Meridian 1 Node can use the authcode conditionally last feature, provided that these systems transmit or repeat all digits dialed by the users in response to the authcode request. This feature cannot be used by certain systems that operate in senderized mode. Correct operation may require adjustment of EOD time-out on systems that employ simulated cut-through operation.

In a private network consisting of multiple switches equipped with the Authcode feature, authcodes should be requested only once on a given call. This requires careful engineering of

— the tie trunk group option for authcode prompting

— the minimum FRL values assigned to route lists

In a private network, users at a switch arranged for the Uniform Dialing Plan (UDP) via a dedicated trunk group to a Node can use the authcode conditionally last feature at the Node in the same manner as those stations located directly at the Node. However, these users cannot access the authcode via the same trunk group after the SPRE feature is activated.

Feature interactions

Feature key operations

While a user is entering an authcode, the following feature keys operate as intended and do not affect operation of the authorization code feature:

— Make Set Busy

— Buzz

— Volume Control

The operation of the following keys is ignored during authcode operation:

— Conference

— Override

— Call Forward and Call Transfer

— Call Pickup

— Charge Account

— Calling Party Number

— Privacy Release

— Ring Again

— Barge-In and Busy Verify

— Speed Call

— Recall

— Do Not Disturb

— Digit Display

The following key operations abort the authcode operation and any digits entered in authcode are ignored:

— Directory Number

— Paging

— Voice Call

— Not Ready

— In-Calls

— Call Waiting

— Hold

— Release

If the caller initiates a switchhook flash while entering an authcode, the results are unpredictable; the switchhook flash may be ignored or interpreted as the digit "1."

Authcodes after SPRE can be stored as speed call or autodial entries. When this is done, the stored number (entry) must contain only the access code and authcode digits. All digits in the entry after the access code are interpreted as authcode digits.

In the case of authcode conditionally last, authcodes can be stored as autodial entries but not speed call entries. If necessary, the caller can continue to enter more authcode digits after operation of the autodial or speed call key. However, for security reasons, authcodes should not be stored as autodial or speed call entries.

Call Detail Recording

If the CDR of authcodes is specified, a record is generated on the CDR device each time an authcode is entered. The record is passed to CDR only if one of the following occurs:

— The call becomes established (for example, a trunk is seized or local telephone answers).

— The call cannot be completed (for example, when no trunks are available).

— The Ring Again feature is applied to the call.

Authcode input via tie trunks

Authcodes can be entered via access tie trunks. Incoming or two-way tie trunk groups at a switch equipped with the Network Authorization Code feature can be defined to prompt the user for an authcode entry.

Direct Inward System Access

If a caller makes a NARS, BARS, or CDP call in association with a valid DISA call, the NCOS associated with the DISA DN is used for NARS, BARS, or CDP route selection. If the FRL of this NCOS is too low to access the route list that NARS, BARS, or CDP has selected for the call, the caller will be prompted for an authcode entry, unless an authcode (for example, Authcode after SPRE) was entered previously.

Barge-In or Busy Verify

If the attendant uses Barge-In or Busy Verify to break into a connection where an authcode is being entered, the authcode entry will be affected. If the code entered is invalid as a result, the user will be given overflow tone when the EOD timer expires.

Centralized Attendant Service

The Centralized Attendant Service (CAS) feature enables several remote switches to share the attendant services at one central location. A CAS attendant can enter an authcode via a Release Link Trunk (RLT), before connecting or transferring calls to the connecting remote PBX. If the CAS attendant enters a NARS, BARS, or CDP number via an RLT, the NCOS associated with the attendant (at the remote PBX) is used in the NARS, BARS, or CDP route selection process. If the FRL of this NCOS is inadequate, the CAS attendant may be prompted for an authcode entry.

Call Forwarding

The Call Forwarding feature provides two customer options: Call Forwarding-Originating (CFO) Party's COS or Call Forwarding-Forwarding (CFF) Party's COS. With the NAUT feature and the CFO option, a caller may be prompted for an authcode entry after a call to a station that forwards the call to a NARS, BARS, or CDP number. With the CFF option, the user will not be prompted by the local switch for an authcode entry after such a call.

Network Class of Service

An authcode entry modifies the user's NCOS for the duration of the call. The FRL associated with the user's assigned NCOS is used to determine if it is necessary to prompt for an authcode entry. After an authcode is collected and validated, the NCOS associated with the authcode is used for the duration of the call.

Network/Basic Alternate Route Selection

During NARS/BARS route selection, the FRL associated with the call originator's NCOS is compared with the FRL of the selected route list. If the originator's FRL is lower and no authcode was entered previously, the system may prompt for an authcode entry. A valid authcode modifies the originator's NCOS and, hence, FRL. This new FRL is then used for route selection.

Network Queuing

When an authcode is entered, the NCOS associated with the authcode is used to determine Network Queuing capabilities.

Coordinated Dialing Plan

Authcode after SPRE can be used before dialing a CDP call. If the NAUT feature is equipped, the "conditionally last" request for an authcode entry applies.

Implementation

Reference list

The following are the references in this section:

- *X11 Administration (553-3001-311)*

This section describes the implementation steps for Basic and Network Authorization Codes. Refer to the *X11 Administration (553-3001-311)* for a complete description of these procedures.

The following responses to prompts in LD 88 are required. Default responses appear in parentheses.

Table 1
Authcode data block (AUB) (Part 1 of 2)

Prompt	Response	Comments
REQ	NEW CHG PRT	Action request (create, modify, or print)
TYPE	AUB	Authcode data block
CUST	0-99	Customer number
SPWD	xxxx	Secure data password
ALEN	1-14	Number of digits in authcode
ACDR	YES NO	Activate CDR for authcodes
RANR	0-511	RAN route number for 'Authcode Last' prompt (NAUT)

Table 1
Authcode data block (AUB) (Part 2 of 2)

Prompt	Response	Comments
CLAS	(0)-115	Classcode value assigned to authcode (NAUT)
COS	aaa	Class of Service
TGAR	(0)-31	Trunk Group Access Restrictions
NCOS	(0)-99	Network Class of Service
AUTO	YES NO	Automatically generate authcodes
_SECR	0-9999	Security password (NAUT)
_NMBR	1-9999	Number of authcodes to be generated automatically (NAUT)
_CLAS	(0)-115	Classcode value assigned to authcode (NAUT)

Table 2
Delete Authcode data block

Prompt	Response	Comments
REQ	OUT	Action request (remove data)
TYPE	AUB	Authcode data block
CUST	0-99	Customer number
SPWD	xxxx	Secure data password
CODE	xxxx	Authcode (number of digits must equal ALEN)
CLAS	(0)-115	Classcode value assigned to authcode (NAUT)

Table 3
Authcode table entries

Prompt	Response	Comments
REQ	NEW CHG PRT	Action request (create, modify, or print)
TYPE	AUT	Authcode entries
CUST	0-99	Customer number
SPWD	xxxx	Secure data password
CODE	xxxx	Authcode (number of digits must equal ALEN)
CLAS	(0)-115	Classcode value assigned to authcode (NAUT)

Table 4
Delete Authcode table entries

Prompt	Response	Comments
REQ	OUT	Action request (remove data)
TYPE	AUT	Authcode entries
CUST	0-99	Customer number
SPWD	xxxx	Secure data password
CODE	xxxx	Authcode (number of digits must equal ALEN)
SECR	0-9999	Security password (NAUT)

To activate or deactivate Station Specific Authorization Codes at a particular telephone, you use LD 10/LD 11:

Table 5
LD 10/LD 11—Activate SSAU

Prompt	Response	Comment
REQ	NEW CHG	Add or modify
TYPE	xxxx	Telephone type: 500 (500 or 2500) 2006, 2008, 2009, 2016, 2018, 2112, 2216, 2317, 2616, 3000, SL1
CLS	(AUTU)	Authcode unrestricted
	AUTR	Authcode restricted
	AUTD	Authcode denied
MAUT	(NO) YES	Modify assigned authcodes for this telephone
SPWD	xxxx	Correct security password (if one is defined)
AUTH	x nnnn	x is in the range of 1-6; nnnn is the assigned authcode (a valid authorization code defined in Overlay 88).
	X	Entering an uppercase X deletes an assigned authcode.
Note: Changing an AUTR telephone to AUTU or AUTD clears all assigned authcode information previously defined for that telephone.		

Table 6
LD 20—Station print

Prompt	Response	Comment
REQ	PRT	Print command
TYPE	xxxx	Type of Terminal Block
TN	l s c u	Terminal number
CDEN	xx	Card density
CUST	xx	Customer number
SPWD	xxxx	Security data password

Note: SPWD is not prompted if any of the following is true:

— The Station Specific Authcode package (220) is not equipped.

— The response to the TYPE prompt is not TNB, SL1, 2000, 2003, 2009, 2018, 2112, 2317, 3000, ARIES, 2006, 2008, 2016, 2216, or 500.

— The response to the TN is more than one specific TN.

— The response to the TN prompt is a unique TN, but the customer of this TN does not have a security data password defined.

— The response to the CUST prompt is not a specific customer.

— The response to the CUST prompt is a specific customer number, but the customer does not have a security data password defined.

Table 7
LD 81—Feature print

Prompt	Response	Comment
REQ	1ST	List sets with the feature specified
	CNT	Count sets with the feature specified
CUST	xx	Customer number
FEAT	AUTU	Authcode unrestricted
	AUTR	Authcode restricted
	AUTD	Authcode denied

Feature operation

Authcode after SPRE

500/2500/SL-1 or digital telephones

To enter an authcode after the Special Prefix (SPRE), the caller proceeds as follows.

— If there is no call in progress, go off-hook or press a Directory Number (DN) key. If there is a call in progress, switchhook flash (500/2500 telephone) or press the call transfer or conference key (SL-1 or digital telephone) to obtain special (interrupted) dial tone.

— Dial the authcode access number (SPRE and the digit "6"). Dial tone is removed after the SPRE digit is dialed.

— Dial the authcode digits. A second dial tone is heard if the authcode is valid. If the authcode is invalid, no response is given for 30 seconds. Then the overflow tone is given for 15 seconds and the call is force disconnected. For more information about how invalid authcodes are handled, refer to "Invalid authcodes" on page 80.

— When the second dial tone is heard, dial the call in the normal manner. If call transfer/conference is in effect, complete the transfer/conference as normal.

Attendant

To enter an authcode after SPRE, the attendant proceeds as follows:

— If there is a call on the source loop, proceed to the next step. If there is no call on the source loop, press an idle loop (LPK) key.

— Dial the authcode access number (SPRE and the digit "6"), followed by the authcode.

— Dial as usual after receiving dial tone denoting a valid authorization code. (If the code is invalid, overflow tone is returned immediately.)

Authcode conditionally last

The following procedure is used to enter an authcode conditionally last from a 500/2500/SL-1 or digital telephone or attendant console (NAUT feature only).

— Dial a NARS, BARS, or CDP call.

— Receive an "authcode request tone" (10 bursts of dial tone, followed by steady dial tone), optionally preceded with a recorded announcement, indicating that an authcode entry is required.

— Dial the authcode. The dial tone is removed after the first digit is dialed. If the authcode is valid, the call is processed as a normal call. If the authcode is invalid, no response is given for 30 seconds. Then the overflow tone is given for 15 seconds and the call is force disconnected. For more information about how invalid authcodes are handled, refer to "Invalid authcodes" below.

Invalid authcodes

When an invalid authcode is entered, the reorder tone occurs after the interdigit time out. (Interdigit timeout is set by prompts DIDT or DIND in LD 15.) The authcode feature does not give the overflow tone immediately upon detecting an invalid authcode to prevent repetitive attempts. However, the network authcode feature (with the NAUT package) does return the overflow tone to the local originating attendant after the attendant enters an invalid authcode with the correct number of digits.

On a tie trunk, entering an invalid authcode locks out the line.

Packaging

Basic Authorization Code is available as package 25.

Network Authorization Code is available as package 63.

Station Specific Authorization Codes are available in package 229. Package 229 requires package 25.

List of terms

AUTD

Authcode denied class of service

AUTR

Authcode restricted class of service

AUTU

Authcode unrestricted class of service

BARS

Basic Alternate Route Selection

BAUT

Basic Authorization Code

CAS

Centralized Attendant Service

CDP

Coordinated Dialing Plan

CDR

Call Detail Recording

CFO

Call Forwarding-Originating

CFF

Call Forwarding-Forwarding

COS

Class of Service

DISA

Direct Inward System Access

DN

Directory Number

EOD

End-of-Dialing

FRL

Facility Restriction Level

NARS

Network Alternate Route Selection

NAUT

Network Authorization Code

NCOS

Network Class of Service

RDB

Route Data Block

RLT

Release Link Trunk

SSAU

Station Specific Authorization Code

SSP

Special Service Prefix

TGAR

Trunk Group Access Restriction

TLD

Toll Denied class of service

Index

Numerics

2500 telephones
authcodes after SPRE with, 79
SSAU in, 10
500 telephones
authcodes after SPRE with, 79
SSAU in, 10

A

ACDR prompt, 73
Activate SSAU prompts, 76
administration, authcode, 61
ALEN prompt, 73
attendant authcode input, 63
after SPRE, 80
AUB (Authcode data block) prompts, 73
AUTD (AUThcode Denied) access level, 10
AUTH prompt, 76
Authcode table entries, 75
authcodes
administration, 61
after SPRE, 79
attendant input, 63, 80
conditionally last, 62, 65, 80
creating, 61
exemptcodes for, 61
invalid, 80
request tones, 62
station specific, 10
validation, 10
Authorization Code Data Blocks, 61
AUTO prompt, 74
autodial entries, 68
AUTR (AUThcode Restricted) access level, 10
AUTU (AUThcode Unrestricted) access level, 10

B

Barge-In or Busy Verify, 69
BARS (Basic Alternate Route Selection), 9, 62, 70
BAUT (Basic Authorization Code), 9
authcode administration in, 61
authcode validation in, 10
documentation, 8
packaging, 81
SSAU in, 10

C

Call Forwarding, 70
CAS (Centralized Attendant Service), 70
CDEN prompt, 77
CDP (Coordinated Dialing Plan), 9, 62, 71
CDR (Call Detail Recording), 63, 69
Centrex systems, 65
CFF (Call Forwarding-Forwarding), 70
CFO (Call Forwarding-Originating), 70
_CLAS prompt, 74
CLAS prompt, 74, 75
classcodes, 61
CLS prompt, 76
CODE prompt, 74, 75
conditionally last authcodes, 62, 65, 80
COS (Class of Service), 61
COS prompt, 74
CUST prompt, 73, 74, 75, 77

D

default facility restriction levels, 62
Delete Authcode data blocks, 74
Delete Authcode table entries, 75
digital telephones
    authcodes after SPRE with, 79
    SSAU in, 10
DISA (Direct Inward System Access), 9, 63, 69
DN (Directory Number), 63

E

EOD (End-of-Dialing) timer, 10
exemptcodes, 61

F

FEAT prompt, 77
feature interactions
    Barge-In or Busy Verify, 69
    BARS, 70
    Call Forwarding, 70
    CAS, 70
    CDP, 71
    CDR, 69
    DISA, 69
    feature key operations, 67
    NARS, 70
    NCOS, 70
    Tie trunks, 69
FRL (Facility Restriction Level), 62

I

ignored keys in authcode input, 67
implementation
    AUB, 73
    Authcode table entries, 75
    Delete Authcode data blocks, 74
    Delete Authcode table entries, 75
    LD 10/LD 11, 76
    LD 20, 77
    LD 81, 77
interdigit timeout, 80
invalid authcodes, 80

L

LD 10 program, 11, 76
LD 11 program, 11, 76
LD 16 program, 62
LD 20 program, 77
LD 81 program, 77
LD 86 program, 62
LD 88 program
    with SSAU, 11

M

MAUT prompt, 76

N

NARS (Network Alternate Route Selection), 9, 62, 70
NAUT (Network Authorization Code), 62
    attendant authcode input in, 63
    conditionally last authcode option in, 62
    documentation, 8
    packaging, 81
NCOS (Network Class of Service), 70
    conditionally last authcodes with, 62
    in classcodes, 61
NCOS prompt, 74
Network Queuing, 70
_NMBR prompt, 74

O

operating parameters, 10, 65
overflow tone, 10, 79

P

packaging, 81
PBX systems, 65
prompts
    AUB, 73
    Authcode table entries, 75
    Delete Authcode data blocks, 74
    Delete Authcode table entries, 75
    LD 10/LD 11, 76
    LD 20, 77
    LD 81, 77

Q

queuing, 70

R

RANR prompt, 73
RDB (Route Data Block) program, 62, 63
remote switches, 63, 70
REQ prompt, 73, 74, 75, 76, 77
Ring Again feature, 69
RLB (Route List Block) program, 62
RLT (Release Link Trunk), 70

S

_SECR prompt, 74
SECR prompt, 75
SL-1 telephones, 79
speed calls, 68
SPRE (Special Prefix), 9, 68, 79
SPWD prompt, 73, 74, 75, 76, 77
SSAU (Station Specific Authcode), 10
SSAU (Station Specific Authcodes)
    operating parameters, 10
    packaging, 81
    prompts, 76
Station print prompts, 77
switchhook flash, 68

T

TGAR (Trunk Group Access Restriction), 61
TGAR prompt, 74
Tie trunks, 9, 69
TN prompt, 77
TYPE prompt, 73, 74, 75, 76, 77

U

UDP (Uniform Dialing Plan), 65

V

validation, authcode, 10

X

X11 release 13, authcodes in, 62
X11 release 19, SSAU in, 10

Meridian 1

Basic and Network Authorization Code

Description

Copyright ©1990–2000 Nortel Networks
All Rights Reserved
Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant. This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC rules, and the radio interference regulations of the Industry Canada. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case users will be required to correct the interference at their own expense.
SL-1 and Meridian 1 are trademarks of Nortel Networks.
Publication number: 553-2751-103
Document release: Standard 7.00
Date: April 2000
Printed in Canada

NORTEL NETWORKS

How the world shares ideas.